1. Code that includes symbolic names and is executable in a program execution environment that resolves the symbolic names, the symbolic names including system symbolic names defined in the execution environment and
the code comprising:
one or more obfuscated names that correspond to system symbolic names;
a first association between the obfuscated names and encrypted forms of the corresponding system symbolic names; and
a static watermark that has been added to the code,
the execution environment including a second association of the encrypted forms with information needed to resolve the corresponding system symbolic names, using the first and second associations to resolve the obfuscated names, and using the static watermark to determine authenticity of the code.

2. The code set forth in claim 1 wherein:
the static watermark's value is a digest of the code prior to addition of the static watermark.

3. The code set forth in claim 1wherein the code further comprises:
other obfuscated names that replace names defined in source code from which the code was made.

4. The code set forth in claim 1 wherein:
the code is downloaded to the program execution environment for execution.

5. The code set forth in claim 1, the code further comprising;
an encrypted first key, the first key having been used to produce the encrypted forms of the corresponding system symbolic names,
the execution environment having access to a second key that can decrypt the first key; and
the execution environment using the second key to decrypt the first key and the first key to make the encrypted forms in the second association.

6. An improved class loader that loads a class in a program execution environment in a host computer system, the class being required for execution of a program in the program execution environment and the program including a first association between symbolic names in the program and encrypted forms of symbolic names defined in the class and the improved class loader being characterized in that:

the improved class loader extends the class on execution of the program in the program execution environment by

using the first association and a second association between the encrypted forms and information used to resolve the symbolic names defined in the class to resolve the symbolic names in the program, and

adding a method to the program which determines whether the program has been modified by the host.

7. The improved class loader set forth in claim 6 wherein:

the method is encrypted prior to being added to the program; and

the improved class loader decrypts the method on adding the method to the program.

8. The improved class loader set forth in claim 7 wherein:

the program includes information from which the method determines whether the program has been modified by the host.

9. The improved class loader set forth in claim 6 wherein:

the program includes a static watermark; and

the static watermark is the information from which the method determines whether the program has been modified by the host.

10. The improved class loader set forth in claim 9 wherein:

the static watermark's value is a digest of the program prior to addition of the static watermark.

11. The improved class loader set forth in claim 9 wherein:

The static watermark is at a location in the program that is determined by a key; and

the method has access to the key and uses the key to locate the static watermark.

12. The improved class loader set forth in claim 6 wherein:

the improved class loader has access to an encryption key that was used to produce the encrypted forms in the first association; and

the improved class loader uses the encryption key to produce the second association on loading the class.

13. The improved class loader set forth in claim 12 wherein:

the program includes an encrypted form of the encryption key used to produce the second association; and

the improved class loader obtains the encryption key by using a decryption key to decrypt the encrypted form of the encryption key.

14. A method of protecting a program that is executed in a host computer system from the host, the program being executed in a program execution environment that loads a class, the class being required for execution of the program in the program execution environment, and the program including a first association between symbolic names in the program and encrypted forms of symbolic names defined in the class,
the method being characterized by the steps performed in the class loader of:

making a second association between the encrypted forms and information used to resolve the symbolic names defined in the class, the first and second associations being used to resolve the symbolic names, and

adding a method to the program which determines whether the program has been modified by the host.

15. The method set forth in claim 14 wherein:

the added method is encrypted; and

the step of adding the method includes the step of decrypting the method.

16. The method set forth in claim 14 wherein:

the program includes information which the added method uses to determine whether the program has been modified by the host.

17. The method set forth in claim 14 wherein:

the program includes a static watermark; and

the static watermark is the information used by the added method to determine whether the program has been modified by the host.

18. The method set forth in claim 17 wherein:

the static watermark's value is a digest of the program prior to addition of the static watermark; and

the added method reads the static watermark, recomputes the digest, and compares the recomputed digest with the watermark's value.

19. The method set forth in claim 17 wherein:

the added method uses a key to locate the static watermark in the program.

20. The method set forth in claim 14 wherein:

the class loader has access to an encryption key that was used to produce the encrypted forms in the first association; and

the step of making a second association includes the steps of accessing the encryption key and using the encryption key to produce the encrypted forms.

21. The method set forth in claim 20 wherein:

the program includes an encrypted form of the encryption key that was used to produce the encrypted forms; and

the step of accessing the encryption key includes the step of using a decryption key to decrypt the encrypted form of the encryption key.

22. A method of protecting a program that is executed in a host computer system from the host, the program being executed in a program execution environment that loads a class that is used in executing the program in the program execution environment and the method being characterized by:

steps performed prior to executing the program in the program execution environment comprising

replacing symbolic names in the program that are defined in the class with obfuscated symbolic names corresponding thereto; and

making a first association between the obfuscated symbolic names and encrypted forms of the replaced symbolic names; and

steps performed on executing the program in the program execution environment comprising

making a second association between the encrypted forms of the symbolic names and information required to resolve the symbolic names;

adding a method to the program that determines whether the program has been modified by the host;

using the first and second associations to resolve the obfuscated symbolic names; and

executing the added method to determine whether the program has been modified by the host.

23. The method of protecting the program set forth in claim 22 further characterized in that:

the steps performed prior to executing the program further comprise the step of

obfuscating other symbolic names that are not defined in the class.

24. The method of protecting the program set forth in claim 22 further characterized in that:

the method to be added is encrypted; and

the step of adding the method includes the step of decrypting the method.

25. The method of protecting the program set forth in claim 22 further characterized in that:

the program includes information from which the method can determine whether the program has been modified by the host; and

in the step of executing the added method, the added method uses the information to determine whether the program has been modified by the host.

26. The method of protecting the program set forth in claim 25 further characterized in that:

the steps performed prior to executing the program further comprise

adding a static watermark to the program; and

the static watermark is the information used by the added method.

27. The method of protecting the program set forth in claim 26 further characterized in that:

in the step of adding the static watermark, the location of the static watermark in the program is determined by a key; and

in the step of executing the added method, the added method uses the key to locate the watermark.

28. The method of protecting the program set forth in claim 22 further characterized in that:

the step of making the second association includes the steps of

obtaining a key used to make the encrypted forms in the first association and

using the obtained key to make the encrypted forms in the second association.

29. The method set forth in claim 28 further characterized in that:

the program includes an encrypted form of the encryption key that was used to make the encrypted forms in the first association; and

the step of obtaining the key includes the step of using a decryption key to decrypt the encrypted form of the encryption key.